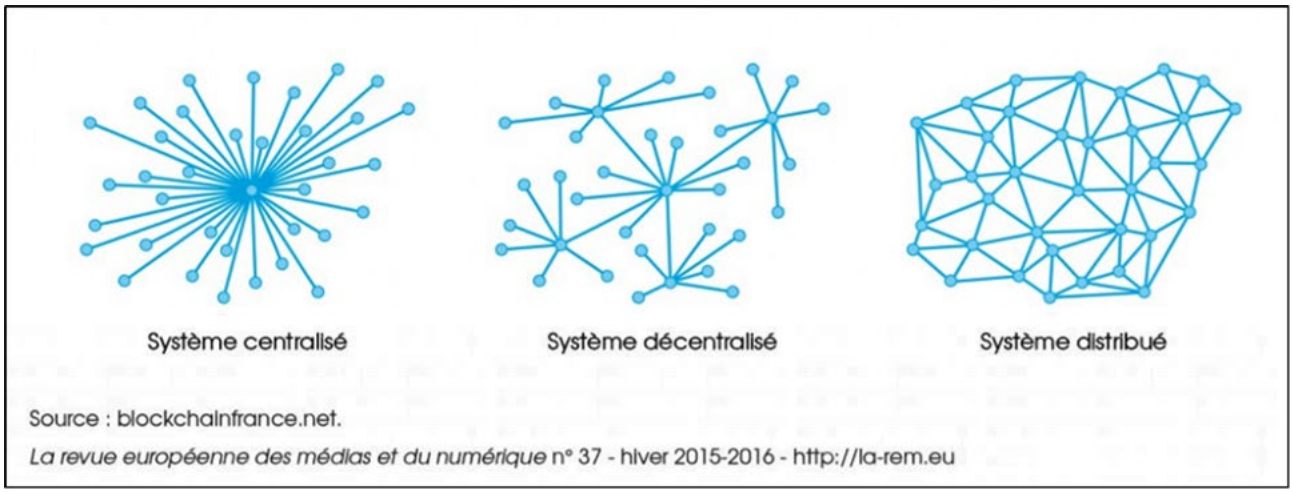
QU'EST CE QU'UNE BLOCKCHAIN ?

François ANDRAULT*
Ingénieur IDN (Centrale Lille)

Au moment où l'on fête les 30 ans du World Wide Web, une application numérique nouvelle se développe rapidement : le concept de *blockchain* s'est fait connaître avec le lancement de sa cryptomonnaie, le *bitcoin*.

Mais d'abord, de quoi s'agit-il et puis, à quoi cela sert-il ?

Avec un *b minuscule*, blockchain est une des technologies préexistantes assemblées pour créer la Technique des Registres Distribués avec un *B majuscule*, la Blockchain est synonyme de cette technique.



La philosophie du système Blockchain, initialement quelque peu libertaire, est de contrôler, garantir, dater et enregistrer durablement des informations entre partenaires, en s'affranchissant de tout contrôle et de toute intervention de tiers, intermédiaire, notaire, banque, état. Dans les habitudes et dans les lois, la BCE ou l'État garantissent la valeur de la monnaie, la banque garantit la disponibilité de fonds lors d'un achat, le notaire garantit la propriété lors d'un échange, etc.
Toutes ces tâches, habituellement assurées par des tiers, seront exécutées par un grand nombre d'ordinateurs, *nœuds* d'un réseau. Le système ne comporte ni administrateur central, ni stockage de données centralisé, il est ouvert à tout le monde ; il n'est pas même nécessaire de s'identifier (on peut utiliser un pseudo).

Le principe de la « **Technique des Registres Distribués ou Partagés** », est de consigner dans un fichier, ou *registre*, l'historique de toutes les informations validées et horodatées que les partenaires désirent garder et préserver. Ces informations ne pourront jamais être modifiées ou supprimées. Ce registre est simultanément enregistré et synchronisé sur un réseau d'ordinateurs ; il se complète par l'addition de nouvelles informations préalablement validées par l'entièreté du réseau. Le registre peut être consulté par tout un chacun, mais pratiquement, il ne peut être ni modifié, ni falsifié, ni détruit.
Satoshi Nakamoto, personne ou groupe, on ne sait pas, aurait créé la Blockchain Bitcoin en novembre 2008.

Quelles sont les principales tâches remplies habituellement par les intermédiaires et que cette technique doit assurer ?

- L'existence de l'émetteur,
- La validation des informations,

* Cet article fait suite à la conférence du 12 mars 2019 de Marc DURAND, ex-responsable de la Blockchain chez IBM (réunion organisée et animée par F. Andrault).

- La fiabilité des transmissions,
- L'existence du destinataire,
- L'horodatage et la pérennité de l'enregistrement des informations.

La Technique des Registres Distribués ou Blockchain doit s'acquitter de toutes ces tâches

Comment être sûr que l'information est vraie et qu'il n'y a pas de substitution d'identité ?

Une fonction mathématique dite de *hachage* cryptographique répond à cette question. Sa propriété essentielle est d'être pratiquement impossible à inverser : l'image d'un message par la fonction (*hach*) se calcule très facilement, mais le calcul inverse, qui consiste à trouver un message à partir de son image, se révèle pratiquement impossible : le temps et les moyens nécessaires pour y parvenir sont beaucoup trop importants. Le *hach* d'un message est unique, et à un hach ne correspond qu'un seul message.
On transmet un message avec son hach et le destinataire, en hachant le message à son tour, peut, par comparaison, s'assurer de la validité de ce message et en même temps de l'identité de l'émetteur.

Peut-on faire confiance au système qui transmet, peut-on être certain que l'information reçue n'est pas falsifiée ?

La sécurité de transmission des données est assurée par cryptographie asymétrique, chiffrement à *clé publique* et *clé privée*. Le destinataire procède à la création d'une transaction, il génère, à l'aide d'un logiciel dédié, une clé publique et une clé privée. Il garde secrète la clé privée et ne la transmet à personne ; il envoie la clé publique au(x) aux émetteur(s). Elle est disponible à toute personne désirant envoyer un message crypté au destinataire.

L'émetteur certifie son identité grâce à un système de signature numérique. Il la joint au message et crypte le tout avec un algorithme de hachage cryptographique utilisant la clé publique : la donnée devient inintelligible à qui ne possède pas la clé privée. Le récepteur l'utilise dans un algorithme de déchiffrement et prend connaissance du message et s'assure de l'identité de l'émetteur.
Le chemin des messages ne passe pas par un organisme de contrôle et de gestion, mais d'ordinateur à ordinateur (*peer to peer*) en respectant un ensemble de règles qui régissent les échanges de données ou le comportement collectif de processus ou d'ordinateurs en réseaux, TCP/IP.

Comment garantir la date et l'enregistrement des messages de manière pérenne ?

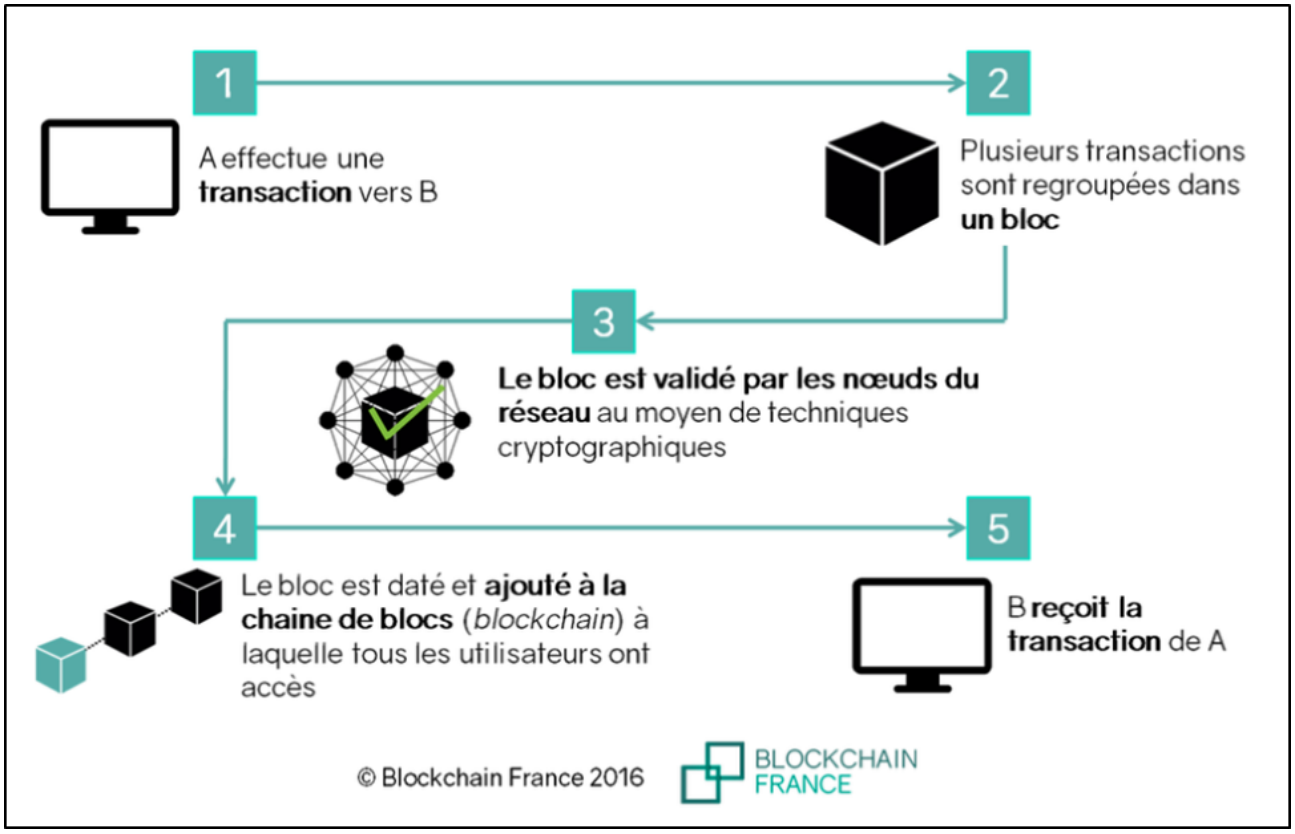
On distribue les informations à tous les nœuds d'un réseau d'ordinateurs. Un *nœud* est un ordinateur détenant une copie d'une blockchain. La plupart des blockchains possèdent entre des centaines et des dizaines de milliers de nœuds.

Un grand nombre de nœuds réseau préserve l'intégrité de la blockchain. Cela permet aux cryptomonnaies d'être insensibles aux tentatives de hack et aux coupures d'électricité. Chacun de ces nœuds est réparti à travers le monde sur des ordinateurs différents. Plus le nombre de nœuds est important, plus le système est sécurisé. Pratiquement, c'est ainsi réalisé pour le *bitcoin*, un destinataire regroupe plusieurs transactions pendant un certain laps de temps (10 minutes par exemple) et les distribue pour validation à tous les opérateurs (nœuds) du réseau.
La véracité des interlocuteurs et la disponibilité des acquis à échanger sont vérifiées grâce à l'enregistrement historique (depuis l'origine du système) de tous les messages. Quand les différentes données sont garanties, l'algorithme de consensus détermine qui enregistrera.

C'est maintenant qu'intervient le concept de blockchain : les messages sont assemblés en un *bloc* qui comporte en outre un entête avec la taille du bloc, le nombre de transactions qu'il contient, la date et l'heure, une somme de contrôles (*hash*) qui empêchera toute modification du bloc et lui servira d'identificateur, et enfin l'identificateur du bloc précédant (sa signature numérique). Le bloc est enregistré dans le registre à la suite de ceux précédemment enregistrés. On ajoute ainsi un maillon à une *chaîne*, d'où le terme *blockchain*, et chaque opérateur reçoit la signature numérique du nouveau bloc.

Nul ne peut altérer l'enregistrement des transactions, car il devrait le faire simultanément sur la totalité des supports sur lesquels il est conservé. De plus, tenter de modifier une information obligerait à modifier toutes les transactions précédentes et tous les détenteurs du registre en seraient immédiatement informés.

Le registre de la blockchain Bitcoin est assez volumineux (actuellement d'environ 120 Go), mais sa signature seule suffit à le garantir.



Toutes ces tâches techniques sont appelées *minage* et les vérificateurs enregistreurs sont dits *mineurs* en souvenir des mineurs d'or. N'importe qui peut devenir mineur, l'inscription, très facile, ne dure qu'une dizaine de minutes. Tous les mineurs reçoivent une copie, une signature, du registre.

Dans le cadre des *cryptomonnaies*, le travail de minage est rémunéré en cryptomonnaie. L'inflation ainsi générée est réglementairement contrôlée et bornée dans le temps. Le *minage* des cryptomonnaies consomme énormément d'énergie électrique, il est donc extrêmement couteux (en 2018 : 400 fois la puissance de calcul de Google). Cela ne peut être durablement toléré (restrictions déjà en Chine). Certaines cryptomonnaies ne sont maintenant plus minées : les « stable coins » comme le *tether* et bientôt le *libra*.

Typologie des blockchains

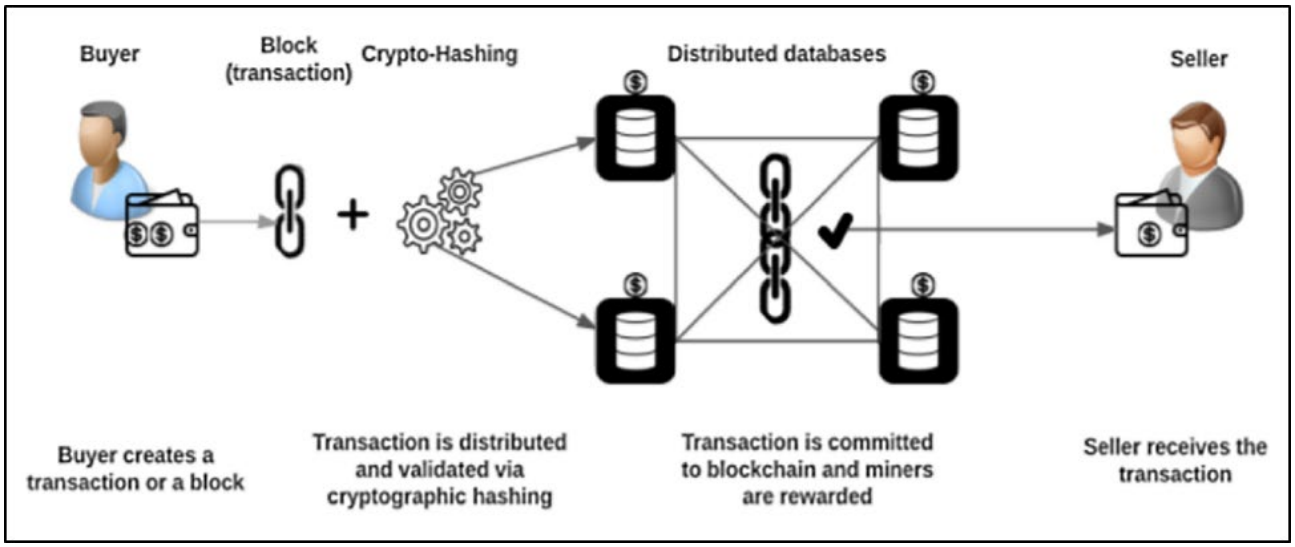
Il existe trois types de blockchain, dont les conditions de fonctionnement varient, ce qui a un impact notamment sur les modes de validation des opérations et donc sur la sécurité des données :
Le droit de lire la blockchain, c'est-à-dire l'accès au registre, peut-être soit public, soit réservé à tous participants du réseau, soit encore réservé à un pool des participants au réseau.

Les *blockchains publiques* (pour les cryptomonnaies) sont ouvertes à tous et accessibles via Internet. La validation des transactions repose sur la notion de « consensus décentralisé », effectuée par ses membres et s'affranchit d'une autorité centrale de contrôle. On y trouve la plupart des cryptomonnaies, dont Bitcoin, Ethereum, et aussi Ripple, Litecoin, Dash ou NEO, etc. Certaines, comme *Ethereum*, permettent les contrats

intelligents - protocoles informatiques qui facilitent, vérifient et exécutent la négociation ou l'exécution d'un contrat ou qui rendent une clause contractuelle inutile.

Les *blockchains hybrides* sont des blockchains dont la gouvernance est partiellement décentralisée entre plusieurs entités qui forment un *consortium* (institutions financières ou entreprises, par exemple). L'accès en est donc limité aux entités membres de ce consortium et la validation des transactions est effectuée par eux sur la base de règles de type « vote majoritaire » : au moins la moitié des acteurs doivent valider les transactions.

Les *blockchains privées* sont, elles, soumises à une restriction d'accès et à une gouvernance centralisée. Les participants d'un regroupement de partenaires peuvent gérer en commun un « processus métier ». Ils se connaissent mais ne se font pas confiance, par défaut ! Pour les rejoindre, les participants doivent être préalablement acceptés par l'entité qui les administre. C'est cette entité centrale qui définit les règles de fonctionnement (droits d'écriture et de lecture) de la chaîne. L'existence d'une cryptomonnaie n'est pas nécessaire pour les blockchains privées.



Quels problèmes pourraient perturber le système blockchain ?

Pour faire, la première fois, une transaction en bitcoins, il faut aller sur un portail spécialisé en services financiers, s'identifier et se créer un portefeuille. On peut ensuite acheter des bitcoins ou toute autre cryptomonnaie sous un pseudo. C'est un bien immatériel protégé par un mot de passe que vous êtes seul à connaître. Vous ne pourrez pas cliquer sur « Mot de passe oublié ? ». En février 2019, un riche milliardaire est mort sans divulguer son mot de passe : l'équivalent de 17 milliards de dollars ont été définitivement perdus et la cryptomonnaie concernée valorisée d'autant !

Cependant, à l'avenir, on peut sérieusement envisager deux problèmes

D'abord l'*ordinateur quantique* remettra le cryptage en question car sa « force brute » sera ultra rapide ! Ensuite, si un groupe de mineurs de connivence dispose de plus de la majorité, il pourrait changer l'utilisation du système ; mais il ne pourrait pas changer les données antécédentes qui seraient préservées.
Les incidents, qui ont été signalés sur le Bitcoin, proviennent de fautes de gouvernance, en amont de la blockchain proprement dite. En 10 ans, il n'a jamais été « cracké ».

On peut reprocher à beaucoup de cryptomonnaies de ne pas avoir de contrepartie matérielle (sauf le *tether* et bientôt le *libra* ; Alipay et WeChat sont adossées à la banque centrale chinoise), mais le dollar non plus pas

de contrepartie matérielle depuis 1971. Les conversions avec les monnaies usuelles réelles sont donc fluctuantes car dépendant essentiellement de l'offre et de la demande.

Les conversions entre monnaies numériques sont, jusqu'à présent, non interopérables.

À retenir parmi les avantages : la Technique des Registres Distribués est un système discret, totalement anonyme, invulnérable, inviolable, rapide, peu coûteux, *business to busines*. Il garantit l'impossibilité de crack financier et pour les cryptomonnaies, un taux d'inflation très faible et diminuant dans le temps.
Dans le cas de blockchain privée, seuls les acteurs autorisés bénéficient d'informations complètes.

Quelles sont les applications de la Technique des Registres Distribués ?

À l'heure actuelle, elle est utilisée dans presque tous les domaines, comme la finance et les transactions internationales, l'énergie, la santé, les industries de fabrication et de transformation, les transports, jusqu'au commerce de détail, etc.

Dans le domaine de la finance, les cryptomonnaies comme le bitcoin, restent partiellement spéculatives, leur valeur fluctue selon l'offre et la demande. Elles servent aussi à des opérations illégales. Une cryptomonnaie assure des transactions sans banque ou organisme de contrôle, d'une personne à une autre, entre sociétés comme entre banques centrales. Elle accélère les processus commerciaux et facilite le suivi et l'automation des règlements. Toutes les grandes entreprises et les banques centrales utilisent aujourd'hui cette technique. Qualité principale : la rapidité.

Dans le cadre de la production et de l'autoconsommation d'énergie électrique d'une collectivité, grâce à la Technique des Registres Distribués, on enregistre en quasi continu la consommation et le cas échéant, la production de chaque client, les frais de gestion, etc. Il n'est plus nécessaire de passer par EDF pour acheter de la puissance électrique à l'étranger. La recharge de véhicules électriques, la gestion de réseaux électriques intelligents, les échanges internationaux de gaz et autres formes d'énergie peuvent faire appel à cette technique. Qualités principales : simplicité, économie.

Dans tous les cas où un seul document doit décrire intégralement, de manière certaine et indiscutable toutes les étapes de vie d'un produit matériel, la Technique des Registres Distribués est ou va être indispensable. On pourra consulter les apports de tous les créateurs, les matériels et produits qui ont concouru à sa création, les incidents de vie, tels que dégradations et maintenance, dates, acteurs, ajouts, les échanges de propriété, jusqu'à la date de destruction et de fin d'existence légale.

Pour le domaine du commerce international, des transports, notamment les transports maritimes internationaux (Maersk), la Technique des Registres Distribués est à l'origine de la création d'une plateforme de renseignement regroupant tous les acteurs de commerce international : commerçants, douanes, autorités portuaires, transporteurs, commerce de détail, etc. Des objets connectés collectent de manière permanente et automatique des données de sécurité (froid). Cela assure, en temps réel, le suivi et la traçabilité de l'acheminement et de la qualité de tout produit transporté.

Dans les industries manufacturières et le commerce, les exemples ne manquent pas, depuis l'enregistrement des brevets, celui des contrats, la protection de la propriété intellectuelle et des biens, la protection de tout ce qui touche aux marques, la traçabilité de tous produits.

La maintenance prédictive des machines et appareillages de sécurité (ascenseurs), la transparence des processus de transformation et du respect des normes de qualité n'est envisageable qu'avec la Technique des Registres Distribués. Un bon exemple est celui de la chaîne du froid : des objets connectés collectent des données de sécurité alimentaire qui sont enregistrés automatiquement et en permanence aux fins de traçabilité. Walmart, avec lequel Carrefour s'est associé, utilise cette technologie. Qualité principale : fiabilité.

Le domaine de la santé offre de nombreuses possibilités d'utilisation de la Technique des Registres Distribués pour certifier, protéger et conserver toutes les données de santé d'une personne : les examens, les analyses, l'historique des maladies et des traitements, les vaccinations, etc.
L'accès aux données peut être limité : par exemple si un généraliste a besoin de toutes les informations, il peut les consulter, mais un kinésithérapeute, par contre, ne reçoit que les informations qui lui sont strictement nécessaires.

Hôpitaux, centres d'analyse, centres de recherche, compagnies d'assurance, laboratoires pharmaceutiques, soignants, patients, sont demandeurs de sécurité pour les données telles que les prescriptions, le suivi de thérapies personnalisées, la certification d'essais cliniques, la véracité et la validation des travaux de recherche, ainsi que pour tracer les médicaments et assurer la sécurité des approvisionnements. Le système aide à lutter contre la contrefaçon (Sanofi venture et Curisium), garantit la passation de marchés et préserve la carte de sécurité numérique de toute fraude.

Pour certifier la propriété, la réalité d'acquisitions, l'identité d'objets, et surtout de personnes (d'immigrés par exemple), on peut enregistrer définitivement, de manière infalsifiable, toutes les données nécessaires, éventuellement jusqu'aux données génétiques, et on ne donnera qu'un accès limité aux stricts besoins de telle ou telle instance.

Une start-up américaine, Everledger, recense 40 attributs des diamants : taille, couleur, pureté, masse en carat, lieu d'extraction, etc., qui constituent 40 métadonnées à partir desquelles un numéro de série unique est créé. Ce numéro de série est ensuite gravé microscopiquement sur la pierre d'une part, et d'autre part ajouté à la blockchain avec les 40 métadonnées. Elle enregistre l'histoire de vie de tous les diamants. Il peut en être ainsi de tous les produits de luxe.

L'acquisition d'un diplôme peut aussi être certifiée et toute personne ayant besoin de s'en assurer recevra le droit d'accès aux données concernées.

La Technique des Registres Distribués protège les droits des créateurs (musiques, bijoux, brevets, etc.).
De même, un reporter peut s'assurer que ses informations ne seront pas altérées ou détruites et se référer à un enregistrement inviolable si contestation.

Une utilisation étonnante dans le domaine de la protection des droits, dans l'immobilier : en Afrique, le cadastre certifié « Technique des Registres Distribués » remplace l'autorité du chef du village !
Des actions similaires sont en cours de réalisation dans le domaine de la propriété foncière en Europe.

Lors d'élections, cette technique peut valider et enregistrer chaque vote (machine à voter électronique) ; il n'est plus possible de pirater ou de truquer des élections. Les informations sont définitivement enregistrées.

Le commerce de détail n'échappe pas aux cryptomonnaies stables (Alipay et WeChat : 800 millions d'utilisateurs). On commence à les utiliser un peu partout en Europe (BHV, Galeries Lafayette, bureaux de tabac…).

On peut utiliser un simple QR code pour s'identifier. Il est scanné par le smartphone de l'acheteur.
Les monnaies locales africaines ne facilitent pas les achats sur Internet : les cryptomonnaies sont bienvenues. Qualité principale : simplicité.

Dans le domaine de la défense et l'échange d'informations c'est le modèle de la blockchain privée qui correspond le mieux.

L'armée française étudie l'automatisation d'une procédure d'interconnexion des Services d'Information

L’armée de l’air américaine (USAF) cherche à mettre en place une blockchain pour sécuriser diverses sources de données dans le cadre de ses opérations de défense.
La Defense Advanced Research Projects Agency (DARPA) a lancé en 2016 un projet de messagerie sécurisée, sans serveur central, qui offre à l’armée américaine un moyen d’échanger des données cryptées rapides en développant un *code « inachable »*. Qualité principale : sécurité.

Conclusion

Encore considérée avec beaucoup de méfiance à cause de débuts tumultueux, la technique blockchain se développe à une vitesse fulgurante et se révèle maintenant indispensable dans de nombreux domaines informatisés. Rien que dans la finance, début 2019, elle atteint 285 milliards de dollars de capitalisation (supérieure à VISA) et les transactions journalières sont de l’ordre de 30 milliards !

Cette importance devient si grande que les états commencent s’en inquiéter : Facebook termine la mise au point en Suisse du *libra*, une monnaie garantie par la capitalisation des ses adhérents (2,5 milliards de clients potentiels, connus, utilisant Facebook, Instagram et WhatsApp). Il dépasse les possibilités financières et de contrôle de nombreux états et, battant monnaie, pourrait en effet être considéré comme tel ! D’où la position dernièrement prise par Christiane Lagarde, présidente de la BCE. Cependant, dans la majorité des cas, on doit considérer l’usage de la technique des registres distribués comme une avancée majeure dans l’administration des biens et le bien être des personnes.